Facebook as a political weapon: Information in Social Networks

David Wills
Research Fellow
Department of Political Science and International Studies
The University of Birmingham
d.a.wills@bham.ac.uk
tel: 07758215739
fax: 0121 414 3496

Stuart Reeves
Research Fellow
Department of Computing Science
The University of Glasgow
stuartr@dcs.gla.ac.uk

Abstract

This paper uses a case study of Facebook to examine the potential use of social networking sites (SNS) for political advantage. Drawing upon contemporary surveillance studies and information technology approaches, it aims to provide insights from these for the study of British politics. The paper uses a model of a constituency election to show the ease and effects of SNS data-mining in support of political campaigning. In doing so, it examines the political implications of machine readable personal data, the design of information systems, and the problems of inductive heuristics and social sorting.

Keywords: Information, Technology, Social Networking, Elections, Surveillance, Computing.

Introduction

Online social networks, or 'social networking sites' (SNS), such as MySpace, Flickr, Twitter and Facebook, have attracted a substantial amount of media attention over the last few years, and are now starting to become the subject of academic inquiry. Their large user bases, the significant amounts of data they produce, and their increasing political impact (Barack Obama acquired 1.5 million friends on Facebook during the recent US presidential election campaign), has unsurprisingly attracted the attention of social and political researchers.

This paper makes use of a hypothetical case study (drawing on real world data) to both highlight and aid discussion of a number of political issues regarding online social networks. The particular online social network discussed is Facebook (www.facebook.com), but many of the conclusions, if not the details of the technical implementation, are applicable to other variations on this theme. Facebook was selected for a number of reasons. Although a number of social networking websites (along with other forms of virtual communities, such as World Of Warcraft and Second Life) have been the focus of much recent interest by the UK media, Facebook offers a number of interesting features beyond its popularity. Users are typically part of geographical networks, are generally identified with their real names rather than pseudonyms, and, crucially, the site contains an explicit reference to 'political views' as part of users' profiles.

In this paper, we make a conceptual distinction between two types of information (or more accurately, two ways of producing knowledge), with differing levels of confidence as to their accuracy, that can be extracted from these networks and then used as a political 'weapon'. These two types are *explicit information* and *implicit information,* and both raise a range of political issues. Explicit data raises issues regarding privacy, intentional and accidental disclosure, human/machine interaction and online social network business models. Implicit data raises issues of relationships and network positions, heuristics, inductive generalisations and probability. We refer to this information as a political weapon due to the potential political use that the data that can be gained from these networks can be put (e.g. compromising the interest of the individual in retaining privacy, or against the interests of an opposing political actor). Many of the issues addressed here are naturally applicable to marketing, and in fact are already used in geo-demographics and targeted marketing strategies, such as those that are being utilised by UK political parties:

> Direct marketing can be a powerful electoral and fundraising tool, identifying voters and matching their preferences with the issues most likely to be of concern, be it rising crime, unemployment or education. It can also help boost membership, a key source of donations (MarketingWeek, 2008).

This paper is not the first place to document security and privacy concerns in relation to Facebook, and in essence this is only the starting point for our discussion (Jones & Soltren, 2005). Because of the ease of creating a profile and of joining networks on Facebook, we take it for granted that information placed on profiles without privacy settings is effectively public to any attacker that wishes to find it and is willing to exert minimal effort. We make use of proof of concept software that shows how very easy it is to perform such data mining operations, even with limited resources. This paper hopes to help bring into mainstream British politics insights from information technology and surveillance research.

This paper should be contextualised against a growing body of research into the politics of surveillance and information technology, and against continuing political developments. Information technology and computer science approaches have introduced a number of insights into surveillance research and will likely continue to do so. Clarke's concept of 'dataveillance' applies to the vast majority of contemporary surveillance. He argued the dominant form of modern surveillance was not visual but rather conducted through mass volumes of personal information, sorted and analysed by computers and held in databases (Clarke, 1991).

The Government is currently pursuing a strongly IT-driven agenda. Bellamy *et al* argue that this arises from a 'modernising' agenda of the Labour government, the

drive to 'join up' the provision of services across government, and the use of preventative risk assessment in social policy – a model that requires processing large amounts of personal data (2005, 134). Concerns about this and other issues led the Information Commissioner to warn that the UK might be 'sleepwalking into a surveillance society' and commissioned a report from the Surveillance Studies Network to examine this (Murakami Wood, 2006). The National Identity Card programme, a programme based upon the government demanding and storing significant data on the population, is still being pursued (Wills, 2008). The recent Communications Data bill incorporates provisions for the retention of the public's communications data, despite removal of plans for this to include a centralised database. The ContactPoint database, intended to safeguard vulnerable children, has entered the first stages of activation, despite fears about its security (Balls, 2009).

At the same time, there is growing attention the use of information technology for purposes of e-democracy including the use of web 2.0 applications – to the extent that almost 100 MPs have Facebook pages. (POST, 2009), Parliament and 10 Downing Street have channels on YouTube.com (www.youtube.com/user/downingst), and the Conservative party host 'webcameron' (http://www.conservatives.com/Video.aspx) signifying the increasing importance being placed upon such systems as sources, sites, and media for political communication. The key difference between such technology and previous channels of communication, such as TV and print media, is the promise of two-way communication, lack of mediation by external interests, and that it has a potentially decentralised nature. Both these trends should draw attention to the personal information and communication channels contained in online social networks, and how this might have political implications, which we attempt to investigate in this paper.

Case study (Part One)

Imagine a political constituency in a parliamentary democracy, with an electoral system something like the UK's. We imagine two main political parties, one 'Red' and the other 'Blue'. This constituency is about to undergo an election, at which both parties have a change at winning. Red has traditionally won this constituency, but on slim majorities. Blue wishes to win this constituency but has limited resources to spend on political campaigning. Because of this they need to target efficiently, ideally based on decent information about who is likely to react well to political advertising or attempts at recruitment and fundraising. Imagine that this constituency has a significant Facebook population (perhaps there is a university).

The Blue party wants to find as many people as possible who have similar political views. Because of the US origin of Facebook (until it recently became fully editable), its political spectrum runs from Very Conservative to Very Liberal. This meant that this type of attack would only work in the UK for the Conservative Party, and certainly not for any socialist or green party. This is what leads many Facebook users in the UK to put 'other' to describe their political perspective. Let us say, then, that Blue are 'conservative', but that they could try and get voters from 'very conservative' and 'moderate' as well. Realising that the 18-24 age group are the demographic group currently least likely to vote (Electoral Commission, 2005), but a group that are highly represented on Facebook, Blue anticipates that there are votes to be gained in this demographic, and therefore decides to undertake some Facebook data mining. There a number of steps from here:

[Figure One here]

The Blue party makes use of some data collection software (such as Panopticon)[i]. The software firstly browses through pages on a given network, collecting the user ID of each member of the network, creating a graph of nodes and edges where 'friend' relationships exist between users. Secondly the software populates a database of profile information collected by accessing the Facebook Application Programming Interface (API), requesting data on each user ID in the graph. If the user's privacy settings allow it then that data will be 'scraped' from the profile (note that should the API deny access, there is always the possibility of collecting information by other, non-official means). The specific data the Blue party are interested in are names, contact information and the contents of the profile field 'political views'. Figure 1 visualises a small section of the dataset collected. In the diagram white nodes represent network members without 'political views' data available, black nodes represent members with conservative, very conservative or moderate as their stated view, and grey nodes represent members whose views are *not* conservative, very conservative or moderate.

Using the database, Blue can generate a list of real names of people, geographically linked to a constituency who have self-identified as conservative, very conservative or moderate. From here, Blue can either query the database for any collected contact information from Facebook profiles (physical addresses or email addresses), or, if they were prepared to try virtual communication, they could send these people messages through Facebook itself – how effective that would be is an area for other research, but unexpected and uninvited communication would likely be considered 'spam'. Additionally, they could cross-reference this list of conservative names with other data such as the electoral roll to find people who were registered to vote. This filtered list allows these individuals to be targeted with campaigning material to which they are likely to be responsive, thereby reducing wastage. The effort is not to win

people over, but largely to remind them to vote; hopefully increasing turnout of the Blue party's likely supporters. Address information may be accessible on the profiles of some users, but this is likely to be less common the more privacy concerns develop. It does however allow targeting of individuals with political sympathies, but who are not yet registered to vote, an especially important consideration with regard to young people and students.

Through intelligent use of very simple data-mining techniques aimed at online social networks, the Blue party attempts to refine their election campaigning, and increase their share of the vote at the election; aiming for a win in this narrowly contested constituency.

Implications – Explicit Data

There are a number of questions raised by this example. Why do individuals disclose such information? What role does privacy, or privacy settings play in this disclosure? And of what importance are levels of disclosure to those running online social networks? Another question of concern here is why people disclose personal data on online social networks. For this, there are a number of potential reasons, based upon the decisions of the users. Use of Facebook, or other social networks is voluntary, so reasons must be provided for why people join in the first place, as well as why people are willing to disclose large amounts of personal information.

Individual reasons for disclosure

The standard information security approach to this question would be to suggest that users are stupid, and are foolishly disclosing more information than would be advisable on the grounds of information security, due to the threat of identity theft, data mining or stalking. This is a standard approach of both privacy campaigners and

security specialists. The latter often display a condescending approach to users, prioritising security over all other concerns and interests. They suggest that users are not aware of privacy settings, or do not know how to use them, or do not realise why they shouldn't publish all this private data. However, whilst there may be users in this category, this account ignores the many and varied reasons that users may have for making use of a service like Facebook. A detailed account would probably require qualitative research into Facebook users and even then is unlikely to be comprehensive (Acquisti & Gross, 2006). Nonetheless, we could anticipate some potential uses (self advertising, finding out about other people, maintaining contact with social circles, finding old friends with whom contact has been lost, and so on) simply to show that there are purposes, and that information disclosure can be regarded as part of the price for those services. A useful addition at this point would be 'presentation of self', a sociological position drawn from Goffman, which suggests that online social networks, and especially the profile, are used to present a particular image to a social environment. Additionally, not all users actively care about disclosing personal information. It increasingly appears that being ever-connected to others in the network plays an important role, and, for many people, is increasingly being seen as a normal, or taken-for-granted aspect of daily life (Hardey, 2007). The information security approach therefore lacks nuance with regard to SNS information disclosure. This approach also appears to form the basis for government efforts to encourage information security through education (www.getsafeonline.org).

A more nuanced approach is drawn from studies of Human-Computer Interaction (HCI). Instead of assuming that people are stupid, certain areas of HCI typically take the view that a good design of the underlying system, and the interface to that system, is essential, and that it is usually poor system and interface design that creates errors or undesirable outcomes during use (including loss of information or privacy). Often,

assumptions about what within a given system is revealed and made accountable to the user help to fuel such design problems (Suchman, 1987). Understanding the process of revealing personal information in terms of interaction with a machine thus offers a potentially useful insight, and indeed, security and privacy design have recently come under scrutiny by researchers from this perspective (Balfanz et al, 2004). However, the database that collates personal information is *not* made visible or made accountable to the user, but rather exists behind-the-scenes as a 'backend'. Even if the user is aware of the existence of the database (and it may not even have existed when they first entered their data on Facebook – as in the example of the Blue party's software), they do not know how it aggregates data, and do not know what algorithms and classifications are applied to the data by its processors.

But this raises a secondary question – why does there exist a place where such information is being disclosed in the first place? Can there be an online social network designed to minimise personal information disclosure? There is, in this respect, a need to move beyond the level of individual decisions and rationality to a study of the structural environment in which disclosure of personal information occurs. We identify two factors that encourage the disclosure of personal information, firstly disclosure to the service itself, and secondly, disclosure to other users.

Firstly, there is an extensive market for personal information (Garfinkel, 2001; Evans, 2005; 6, 2005). Personal data is valuable data for data mining purposes and for re-sale to interested parties, not least to the numerous data warehouses that buy up and aggregate data sets. This is used for direct marketing, consumer profiling and the targeting of services. Facebook, and other social networking sites, are valuable sources of such data. This is especially significant in the case discussed here, in that Facebook users are often identified by their real names. Additionally, as data is revealed to friends to facilitate interaction, and is therefore subjected to accuracy

checks by people who know the subject offline, this data is likely to be of much higher quality than that produced by market research surveys or telephone polls per se (Donath and Boyd, 2004: 73).

Facebook's Privacy policy explicitly states that the company is willing to pass on the data posted by users on to third parties:

> Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or film and personalising advertisements and promotions so that we can provide you with Facebook. (http://www.facebook.com/policy.php).

However, the provision of these services is not incompatible with systems that place a higher value on privacy. These needs could also be met, for instance, by a system in which information revealed to the social networking service was then encrypted, and kept hidden from any other prying eyes (like the Blue party), and being sold on only to those that met the asking price. Facebooks's policy thus raises several interesting questions concerning the availability of user information, not least that of why there is even a setting for 'political views', and why Facebook's privacy settings are not set at their highest by default. A potential answer to these questions is the structural motivator behind the online social networking model that encourages disclosure and the reduction of control over personal information. In short, the system is set up in such a way that *encourages* information disclosure.

Structural reasons for disclosure

According to 'Metcalf's Law' the utility of a network is equal to the square of the number of users (O'Hara & Stevens, 2006:38-9). Put simply, the more users that a network has, the more useful it is. Note that this law does not say *who* the network is

useful for. Network utility increases for users because they are more likely to find their friends on Facebook if more people are members. Network utility increases for the owners of Facebook because they have more people to gather data from, more people to advertise to, and a more useful network for users that will cause more people to join, or keep people using the service. It is this size and growth that resulted in Facebook being valued at $15 billion when Microsoft invested $240 million for a two per cent share in October 2007. Network utility also increases for outside agents who want to data-mine the network – although this may be a more linear than exponential increase.

This is important because the business model of online social networking sites seems to involve the need to grow as large a user base as possible, hence the exhortations to find more friends and expand your network ad infinitum. Part of the reason that Facebook is valued so highly is because of its expanding membership figures. In many ways, a useful analogy is that of newspaper publishing. Newspapers do not get the majority of their profit from the cover price of the paper. They get their profits from selling an audience (their readers) to advertisers. In a sense, online social networks have made an advance on this model – they do not even need to provide any content, as 'content' is provided by the users themselves as they network, post information and communicate with each other. Another well noted feature of online social networks is that they also exhibit a tendency to die off, as users find little use for a service once they have established a network (Donath & Boyd, 2004). To minimise this problem, networks have an incentive to encourage users to produce as much content as possible – in essence, to reveal as much data as possible to other users. This is why privacy settings are by turned off by default when a user signs up to a Facebook account. Disclosure is required to make the network attractive.

Some parallels can be drawn from real world social networks. Gossip, 'the process of informally communicating value-laden information about members of a social setting' (Noon & Delbridge, 1993), or personal information disclosure between members of a shared social network, can be seen as essential to the maintenance of social networks. In both these scenarios, it is of course possible to free-ride on the information disclosure of other members of the network. However, the more significant point is that the incentives of the network users may not be (and are likely not) the same as the network operators. This means that whilst there may be ways to design a more secure network, there are strong incentives for Facebook and similar networks not to do this.

Case Study (Part Two)

The data that the Blue party acquired in Part One was good, and helped them to refine their election campaigning. However, the data is patchy. Some individuals in the target network have either been paying attention to security advice, been scared by media stories of identity theft, or have otherwise changed their attitudes towards information disclosure. As a result they have changed their privacy settings. Either they have set their profiles so that we cannot access their political affiliation if we are not a friend, or perhaps they've simply not filled in the 'political views' field.

[Figure Two here]

However, they have linked themselves to a number of Facebook friends, some of whom have not taken the same attitude to disclosure, and have placed their political orientation on public view. Following the heuristic that political affiliations cluster together, summed in the folk wisdom that 'birds of a feather flock together', The Blue Party make the assumption that people tend to have similar characteristics to their

friends. The software described in Part One can also *recursively* collect data for a given network, retrieving data about any network members' friends, their friends, and so on. Figure 2 provides a graphical overview of a section of data the authors collected from Facebook in August 2007 using the simple program mentioned earlier. This data was sourced from a 'network' one of the authors was a member of, resulting in information from over 1300 individuals being recorded. The same conventions remain for this figure as in Figure 1, except this time friend relationships have been plotted as lines between nodes. In order to enhance visibility, friend relationships (i.e. lines) belonging to conservative nodes have been emphasised. We therefore examine this additionally collected 'deeper' friends data, and can then start to infer what political views an unknown network member might have. This is done by examining the number of friends of such an individual who have self-identified as conservative or very conservative – generating a percentage. Depending on the resources we have to spare, and how deep we wish to go recursively, we can set a *threshold* at which we act as if this unknown network member is a 'Blue' and start to initiate campaign mailing, email, and the like.

For example, if an individual has thirty friends on Facebook, twenty of whom describe themselves as 'very conservative,' 'conservative' or 'moderate,' we have reasonable grounds to guess that this individual's political views would be somewhere in the 'blue' spectrum. Likewise, if an individual had no 'blue' friends, it would be considered unlikely that they would be receptive to Blue party marketing, and they are excluded from the contact list. This concept is illustrated in Figure 3, which shows a closer view of a portion of Figure 2. In addition to white, grey and black nodes, Figure 3 also has nodes marked with a black box. These are members of the network for which the number of conservative friends (whether in the network or not) exceeds

the number of non-conservative friends (again, whether in the network or not) and as such presents a potential target for the Blue party.

[Figure Three here]

The Blue party therefore has made use of the *implicit* information that is in the network, rather than listed on the profiles of any individual users. It is based on position and relationships, and bypasses privacy settings. There are also more nuanced ways in which this could be done. For instance, if an unknown user has unknown friends, we could in turn estimate their probably rating before applying it to our initial unknown (perhaps with a lower probability). Additionally, one could use graph theoretic algorithms in order to weight tightly integrated clusters of friends, as this would be more likely to signify close friends rather than casual acquaintances (to which rules of thumb may be more likely to apply). However, for the *degree of certainty* required for this sort of operation, this is probably unnecessary.

Implications – Implicit Data

This use of inductive logic and simple heuristics, along with the data mining of an online social network raises a number of issues; firstly, concerning the nature of relationships and connections in online social networks themselves, and secondly, concerning heuristics and the perennial philosophical problem of inductive reasoning.

'Friends' as empty signifier

To become friends with somebody on Facebook is a two-part process. Firstly, one user, having found the profile of person they wish to befriend, clicks on a link to 'Add to Friends'. This sends a 'friends request' to the second user, presenting that user with

the choice to ‘accept’ or ‘ignore’ the request. If the second user accepts the request then the users become ‘friends’, being listed on each other’s profile (to an extent determined by privacy settings). ‘Friend’ in this sense is a broken metaphor; individuals linked to each other on Facebook need not consider themselves actual ‘friends’ in a traditional sense, but simply have been willing to accept the request to link. It may be profitable to consider ‘friend’ in this respect as an floating signifier, which can be articulated by users in a number of ways according to their particular discursive construction of their profile. I may use Facebook only to keep in touch with what I consider to be ‘real’ friends, and therefore have around fifty friends to whom I am linked. An undergraduate student may add as a friend pretty much everybody they meet during their three years at university, and may therefore accumulate a list of several hundred. I may be willing to reject or ignore friends' requests from people I do not consider as friends, whilst others may find this behaviour rude. We operate with differing conceptions of what ‘friend’ entails. In fact, we can have multiple articulations of friend in the same list. The problem here is that relationship analysis ignores this, in effect flattening relationships and granting all links in the network equal weight. This may be a structural effect of online social network links which are mutual, public, un-nuanced and de-contextualised (Donath and Boyd, 2004:72). From the perspective of an outside observer, then, all links appear equal, whilst all of them are termed ‘friend’, creating a tendency to apply traditional social models and rules of thumb. The problem arises that I might not consider my friends' political leanings (or sexual orientation, or favourite movies) when I choose to establish a link with them. Technological systems may reduce ambiguity, fixing floating signifiers in unpredictable ways.

Heuristics and the logic of induction

Heuristics are a tool for thinking, or 'rules of thumb'. The rule of thumb that is critical for the Blue party in our case here is the idea summed up by such sayings as 'birds of a feather flock together', and 'judge a man by the company he keeps'. If an individual is part of a group, it is likely that the individual will share some characteristics with other members of that group (other than simply being a member of the group). This is far from a new model of social networks, and highlights how, whilst the technology behind information technology and online social networks may be relatively new, many social concepts (including social scientific theories) can be transferred to this new medium without the need to totally re-invent the wheel. An analogy would be the use of the concept of 'guilt by association' in use by police and intelligence services throughout history. Heuristics are, of course, not always true or accurate. Many have no doubt been falsely imprisoned or disadvantaged on the basis of such assumptions.

This particular form of heuristic is more accurate in highly polarised societies. In a bi-modal society, any given individual is likely to be in one of two groups, with few contacts with members of the other group. Imagine the 'Red' and 'Blue' states in the USA, or Catholics and Protestants in Northern Ireland. Heuristics are reliant upon the philosophical principle of induction.

Induction can be problematic to describe, involving generalisations drawn from specifics, or the extrapolation from a sample to a total population. The strongest critique of inductive logic arises from Hume, which seems to show that there is no logical ground upon which to base induction. However, induction is at the heart of scientific rationality and experimental science (Baggini & Fosl, 2003:7-11). The conclusions of induction can only ever be described in terms of probability, not necessity. A wise user of our system would recognise this. However, there is a political and social problem that emerges in this sort of profiling, in which these profiles become taken as authoritative and used as a basis for decisions that are more

significant than party political advertising, such as the decision to grant or refuse credit. Heuristics are taken as truth when at best they might be crude stereotypes. At some point, gradients, probabilities and uncertainties become binaries.

> People are at risk. The risks are those of mistaken identity, or more seriously, of correctly identified persons whose life-chances and choices and whose freedom to move about or to communicate are jeopardized by their being placed in categories that define them in specific ways (Lyon, 2007:192).

We would be wary of relying on this logic as a form of social science, and this paper does not present this model as one that should be adopted by researchers. It presents this as a method that actors will use, and one that has social and political effects. In many respects, this reflects what Deleuze refers to in the *Postscript to Societies of Control*, a breakdown of sites of confinement combined with modulation of control, the creation of gateways and barriers, which are not always visible to the individual who wishes to pass through them (Deleuze, 2002: 317-321). Individuals can be excluded from opportunities to participate in social life (or included in categories they would rather not be included in) based on inductive decisions based on their data profile (Haggerty & Ericson, 2000: 605-622). Imagine if rather than political affiliation, the same approach was taken towards revealing the sexual orientation of people who wished to keep it private. There is a growing literature on 'social sorting' and the way that classifications and categorisations based upon surveillance and personal data are beginning to have important effects on a range of economic, social and political practices (Gandy, 1996; Lyon, 2003).

> Social sorting increasingly defines surveillance society. It affords different opportunities to different groups and often amounts to subtle and sometimes unintended ways of ordering societies, making policy without democratic debate (Murakami Wood et al, 2006:8).

Conclusions

This paper has attempted to bring insights from surveillance studies and human-computer interaction to the field of British politics, to cast light on contemporary developments in the field of politics of technology and the technology of politics. The main conclusion of this paper is that there is significant personal information to be extracted from online social networks. Even when privacy settings are enacted there are ways to extract information from the structure of the network itself. This has always been possible, but the textual nature of the network databases makes this information more visible and machine-readable. We have shown through a practical example how political decisions can be made on the basis of revealing information, and information extracted from the shape of social networks. We have shown how some of the political implications of data disclosure, and have considered some of the individual and structural motivations for information disclosure, concluding that information system design should play a more important part in protecting privacy, rather than relying on individuals to counter a system's in-built problems through 'correct' behaviour. This is an insight that has relevance far beyond social network design, and should be at the core of any government IT project. We have demonstrated how data disclosure can be understood as interaction with an opaque machine, without knowledge of rules, logics and thresholds that are hidden from view. These findings have political implications that will likely only become more significant as technology and information systems play an increasing role in British political life.

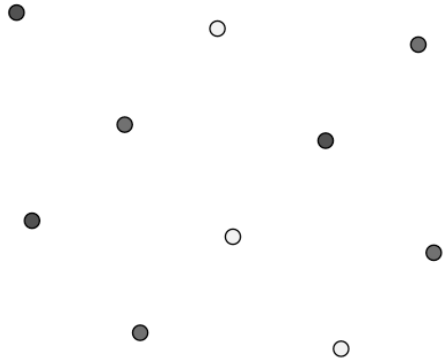

Figure 1: A section of the dataset

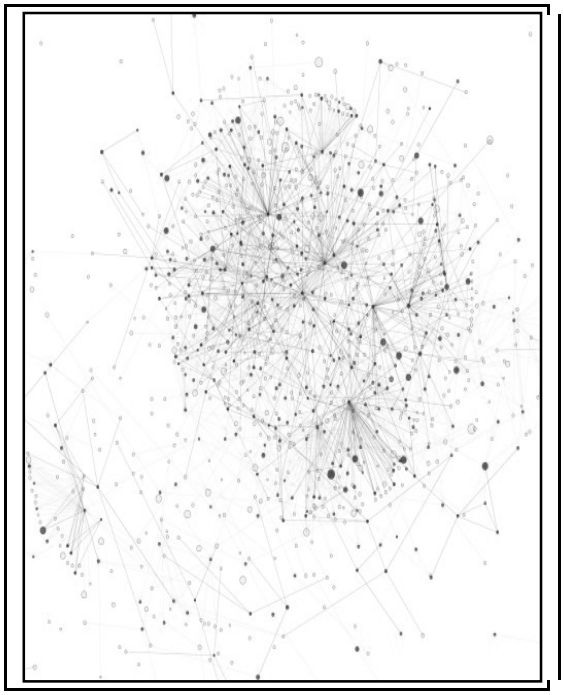

Figure 3: An overview of a section of the dataset

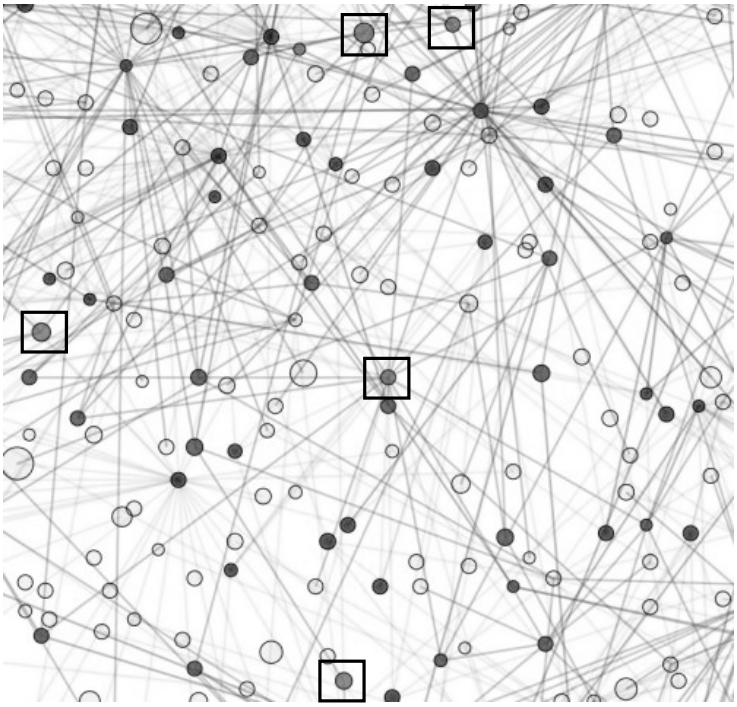

Figure 2: A closer view of the dataset

Bibliography

6, P. (2005) 'The Personal Information economy: Trends and Prospects for Customers' in Lace, S. (ed) *The Glass Consumer: Life in a Surveillance Society*. Bristol, Policy Press.

Acquisti, A. & Gross, R. (2006) 'Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook' *The 6th Workshop on Privacy Enhancing Technologies*. Robinson College, The University of Cambridge, 28/06/06

Anderson, R. & Moore, T. (2006) 'The Economics of Information Security' *Science*, 314, pp.610-613

Baggini, J. & Fosl, P.S. (2003) *The Philosopher's Toolkit: A Compendium of Philosophical Concepts and Methods*. Oxford, Blackwell.

Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K., and P. Stewart (2004) "Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute" in Proceedings of the USENIX Security Symposium 2004. San Diego, California. August 9-13. 207-222.

Balls, E. (2009) *Safeguarding*. Department for Children, Schools and Families. http://www.everychildmatters.gov.uk/_files/DCSF_ContactPoint_WMS_26_Jan_09.pdf

Bellamy, C., 6, P., & Raab, C. (2005) 'Personal data in the public sector: reconciling necessary sharing with confidentiality.' In S.Lace (ed.).

Clarke, R. (1991) 'Information Technology and Dataveillance' in C. Dunlop and R. Kling (eds.) *Controversies in Computing*. San Diego, Academic Press.

Deleuze, G. (2002) 'Postscript on Control Societies' in T.Levin, U. Frohne and P.Weibel, (eds.) [CTRL]Space: Rhetorics of Surveillance from Bentham to Big Brother. Cambrige, Mass & London: MIT Press.

Donanth, J. & Boyd, D (2004) 'Public Displays of Connection' *BT Technology Journa*l. Vol 22 No. 4, October 2004.

Electoral Commission (2005) Election *2005: Turnout. How many, who and why?* The Electoral Commission.

Evans, M. (2005) 'The Data informed marketing model and its social responsibility' in Lace, S (ed.) *The Glass Consumer: life in a surveillance society*, Bristol, The Policy Press.

Facebook (2007) Facebook Privacy Policy <http://www.facebook.com/policy.php> (24th May 2007)

Gandy, O.H. (1996) 'Coming to terms with the Panoptic Sort' in D. Lyon & E. Zureik (eds.) *Computers, Surveillance, Privacy*. Minneapolis & London: University of Minnesota Press.

Garfinkel, S. (2001) *Database Nation: The Death of Privacy in the 21st Century*. Sebastepol, O'Reilly publications.

Goodin, D. (2007) 'How to Sniff Out Private Information on Facebook' The Register, 26th June 2007. <http://www.theregister.co.uk/2007/06/26/sniffing_private_facebook_info/>

Haggerty, K.D. & Ericson R.V. 'The Surveillant Assemblage' *British Journal of Sociology,* Vol. No.51 Issue No.4, December 2000. pp.605-622

Hardey, M (2007) 'Going Live: Converging Mobile Technology and the Sociability of the iGeneration.' Media-Culture. Vol.10. Issue 1.

Jones, H. & Soltren, J. H. 'Facebook: Threats to Privacy' Student term paper, MIT, December 14, 2005. <http://www-swiss.ai.mit.edu/6.805/student-papers/fall05-papers/student-papers.html>

Lyon, D. (2007) *Surveillance Studies: An Overview*. Cambridge, Polity

Lyon, D. (2003) (2003) 'Surveillance as Social Sorting: Computer codes and Mobile bodies' in Lyon (ed). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York, Routledge.

MarketingWeek (2008) 'Perils of Political Fundraising' *MarketingWeek*. 29th October. www.marketingweek.co.uk/cgi-bin/item.cgi?id=63082

Murakami Wood, D.(2007) 'Securing the Neurocity', *Criminal Justice Matters*, no, 68, Summer 2007

Murakami Wood, D. (Ed.) (2006) *A Report on the Surveillance Society: For the Information Commissioner by the Surveillance Studies Network.* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

O'Hara, K. & Stevens, D. (2006) *Inequality.com: Power, Poverty and the Digital Divide*. Oxford, Oneworld.

Parliamentary Office of Science and Technology (2009) 'POSTnote 321: E-Democracy' www.parliament.uk/parliamentary_offices/post/pubs2009.cfm

Privacy International (2007) *Consultation Report: Race to the Bottom.* <http://www.privacyinternational.org/issues/internet/interimrankings.pdf>

Suchman, L.A. (1987) *Plans and Situated Actions: the Problem of Human/Machine communication*. Cambridge, Cambridge University Press.

Wills, D.A. (2008) 'The United Kingdom identity card scheme: Shifting Motivations, Static Technologies' in C. Bennett & D. Lyon (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. London & New York, Routledge.

WORDCOUNT: 6044
DATE: 29/01/09

[i] Available at: http://www.tropic.org.uk/~stuart/panopticon.html. For newer versions used to produce images contained within this paper, please contact the authors.